

---

## Schritte in Richtung Datenschutz

---

Arbeitshilfe  
für digital arbeitende  
Fachkräfte der aufsuchenden  
Jugendsozialarbeit





# Schritte in Richtung Datenschutz



Arbeitshilfe  
für digital arbeitende  
Fachkräfte der aufsuchenden  
Jugendsozialarbeit

## **Inhalt**

- 4 Über diese Arbeitshilfe
- 4 Was ist das Problem?
- 5 Was bietet diese Arbeitshilfe?
- 6 Grundlegendes zur DSGVO
  
- 10 Vier grundlegende Schritte für die datenschutzkonforme Arbeit
- 10 1. Anlegen und Pflege eines Verzeichnisses
- 11 2. Datenschutz-Check vor dem Beginn der Nutzung eines Tools / Dienstes
- 13 3. Anpassung der eigenen Datenschutzerklärung
- 14 4. Datenschutzerklärung und Impressum in Online-Präsenzen aufführen
  
- 14 Hinweise für die Erstellung von Arbeitsprofilen in sozialen und digitalen Medien
- 17 Umgang mit besonders sensiblen Daten
- 19 Selbstschutz der Fachkräfte
- 19 Jugendliche für Datenschutz sensibilisieren
- 20 Fazit

### Was ist das Problem?

Es steht außer Frage, dass Jugendsozialarbeit auch digitale Räume einbeziehen muss, da Jugendliche sich online aufhalten, kommunizieren, ihre Freizeit verbringen und Digitalisierung auch aus Schule, Ausbildung und Arbeit nicht mehr wegzudenken ist. Durch die Corona-Pandemie waren auch Jugendsozialarbeiter\*innen sehr plötzlich gezwungen, einen erheblichen Teil der Arbeit, die vorher in analogen Räumen stattfand, auf Online-Räume zu verlagern. Durch diese plötzliche Intensivierung des Arbeitsbereichs fanden Träger und Fachkräfte vielfältige kreative, neue digitale Lösungen, Ansätze und Angebote – gleichzeitig und in den folgenden Wochen und Monaten zeigten sich dabei allerdings Hürden und Probleme.

Eine zentrale Herausforderung ist der Umgang mit und insbesondere der Schutz von (sensiblen) Daten von Adressat\*innen ebenso wie Fachkräften. Das Kernelement der (aufsuchenden) Jugendsozialarbeit ist die Beziehungsarbeit, die in erster Linie auf Kontakt und Kommunikation aufbaut. Häufig werden sensible oder intime Themen besprochen – in analogen Kontexten geschieht dies oft auf Parkbänken, in einem Beratungsraum, im Jugendzentrum oder außer Hörweite auf dem Sportplatz, um die Vertraulichkeit zu wahren und die Adressat\*innen davor zu schützen, dass ungewollt weitere Personen von den Gesprächsinhalten erfahren. Ebenso ist es in digitalen Kontexten wichtig, sicherzustellen, dass persönliche Daten nicht von Dritten eingesehen werden können. Die Probleme sind hier oft nicht auf den ersten Blick ersichtlich: Viele Jugendliche nutzen Plattformen, die datenschutzrechtlich unsicher sind; versenden Dateien wie Fotos von »gelben Briefen«, die anschließend in Clouds gespeichert werden; teilen ihr Endgerät mit weiteren Haushaltsmitgliedern. Während »Face-to-Face«-Gespräche nicht zu ersetzen sind, ist gleichzeitig klar: es braucht digitale Räume für Gespräche, die ein möglichst hohes Maß an Schutz bieten, um den Raum für Gespräche über Sucht, Schulprobleme, Diskriminierungen, psychische Belastungen, Krankheiten, Gewalt, Ängste und vieles andere mehr in einem ähnlich geschützten Rahmen wie im Analogen zu ermöglichen.

Zentral ist für viele Träger und Fachkräfte die Frage, ob und wie sie für den Kontakt und die Kommunikation mit ihren Adressat\*innen beliebte soziale Medien oder Kommunikationsnetzwerke wie z.B. WhatsApp, Instagram oder Zoom nutzen können. Die Annahme ist häufig,

dass deren Nutzung aufgrund der Datenschutzgrundverordnung (DS-GVO) ausgeschlossen ist, u. a. weil die Server außerhalb der EU betrieben werden und nicht ausreichend vor dem Zugriff durch Externe geschützt sind. Die Nutzung einer eigenen App oder Plattform »nur« für die Kommunikation mit den Fachkräften kommt aber für Klient\*innen und Adressat\*innen oft (zunächst) nicht in Frage. Die Installation einer App oder das Anlegen eines Accounts ist eine deutliche Hürde und kann zu Kontaktabbrüchen oder Kontaktvermeidung führen bzw. schränkt insgesamt die Erreichbarkeit ein. Da die Kommunikation mit den Klient\*innen so zentral ist, müssen auch Wege gefunden werden, beliebte Plattformen und Messenger auf möglichst sichere Art und Weise zu nutzen und somit die niedrigschwellige Arbeit der Fachkräfte in den Lebenswelten der Zielgruppen zu gewährleisten.

Im Rahmen des Projektes »DiMe – Digitale Methoden der (aufsuchenden) Jugendsozialarbeit« fanden eine Fortbildung und ein Fachtag mit Streetworker\*innen unter juristischer Beteiligung statt, um die Herausforderungen, Bedarfe und Interessen von Fachkräften und Klient\*innen zur Kommunikation über unterschiedliche Medien und Plattformen zu erläutern und Möglichkeiten des Umgangs mit (sensiblen) Daten zu besprechen. Ziel war es, Wege einer möglichst sicheren Kommunikation zwischen Streetworker\*innen und Klient\*innen zu erarbeiten. Die vorliegende Arbeitshilfe fasst die erarbeiteten Hinweise zusammen, die einen möglichst umfassenden Schutz der Daten entsprechend der DSGVO und den professionellen Ansprüchen der Jugendsozialarbeiter\*innen mit den Bedarfen und Lebensrealitäten der jugendlichen Zielgruppen zusammenbringen sollen.

## **Was bietet diese Arbeitshilfe?**

Die Arbeitshilfe erklärt sehr komprimiert zentrale Inhalte der DSGVO und deren Auswirkungen auf die praktische digitale Arbeit von aufsuchend arbeitenden Jugendsozialarbeiter\*innen. Sie fasst zusammen, was jede Fachkraft (mindestens) über personenbezogene Daten und deren Verarbeitung wissen sollte. Im Anschluss daran macht die Arbeitshilfe Vorschläge zur praktischen Umsetzung der Vorgaben der DSGVO in der aufsuchenden Jugendsozialarbeit für die Fachkräfte, die (auch) in digitalen Medien mit Jugendlichen arbeiten. Der Fokus liegt dabei auf populären Medien der Adressat\*innen, also bspw. WhatsApp und Instagram.

## Hinweis!

Diese Arbeitshilfe stellt keine Rechtsberatung dar. Für die Vollständigkeit, Richtigkeit und Aktualität wird keine Haftung übernommen. Die Hinweise sollen Trägern und Fachkräften dabei helfen, eigene Konzepte und Strategien zur Einbindung digitaler Kommunikation zu erarbeiten bzw. zu verbessern. Auf die juristischen Grundlagen wird jeweils verwiesen.

## Grundlegendes zur DSGVO

Die DSGVO regelt den Schutz personenbezogener Daten. Was personenbezogene Daten sind, wird im Art. 4, Abs. 1 der DSGVO erklärt. Dieser Artikel definiert insgesamt alle wichtigen Begriffe, die in der DSGVO verwendet werden, also bspw. auch den Begriff »Verarbeitung«.

## Personenbezogene Daten

Im Sinne der DSGVO »bezeichnet der Ausdruck »personenbezogene Daten« alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann,« (DSGVO, Art. 4, Abs. 1)

Durch die Nutzung von sozialen Medien bzw. die Erstellung von Accounts im Internet werden i. d. R. personenbezogene Daten erhoben und verarbeitet.

Auch in der Jugendsozialarbeit werden oft Daten **erhoben**, bspw. in der Beratung oder für die Dokumentation: schon das Notieren eines Namens und einer Telefonnummer ist eine Erhebung von Daten. Zum

anderen passiert die Erhebung von Daten häufig automatisch durch die Anmeldung und/oder Nutzung von bestimmten Plattformen und Tools, über die Jugendsozialarbeiter\*innen mit ihrer Zielgruppe kommunizieren. Die erhobenen Daten werden bspw. in der Jugendsozialarbeit oft **verarbeitet**, um z.B. Statistiken zur eigenen Arbeit aufzustellen oder Freizeit- oder Beratungsangebote machen zu können. Ebenso gehören die Veröffentlichung des Fotos einer Person (z.B. im Internet), die Nutzung einer Kontaktdatenbank mit persönlichen Daten und andere Vorgänge zum Bereich der Verarbeitung. Die Definition des Begriffs »Verarbeitung« aus der DSGVO bietet den Rahmen, um zu identifizieren, wo in der eigenen Arbeit personenbezogene Daten verarbeitet werden. Auch Online-Dienste verarbeiten Daten, um ähnlich wie in der Jugendsozialarbeit z.B. Statistiken aufstellen zu können. Dies passiert ebenfalls häufig automatisch durch die Nutzung bestimmter Plattformen.

### »Verarbeitung«

Im Sinne der DSGVO »bezeichnet der Ausdruck: »Verarbeitung« jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung« (DSGVO, Art. 4, Abs. 2)

Bei einer Erhebung oder Verarbeitung von Daten gibt der Art. 5 DSGVO klare Richtlinien vor, in deren Rahmen der Umgang mit den personenbezogenen Daten stattfinden muss bzw. darf. Dies sind die Grundsätze der Datenverarbeitung:

- **Rechtmäßigkeit;**
- **Zweckbindung**, d.h. Daten dürfen nur für einen bestimmten, offengelegten Zweck erhoben und ggf. verarbeitet werden;
- **Datenminimierung**, d.h. es dürfen nur so wenige Daten erhoben werden wie nötig;
- **Richtigkeit**, d.h. die erhobenen Daten müssen sachlich richtig und auf dem neuesten Stand sein und es muss angemessene Maßnahmen zur Berichtigung und Löschung geben;
- **Speicherbegrenzung**, d.h. Daten dürfen prinzipiell nur so lange gespeichert werden, wie es für den Zweck notwendig ist;
- **Integrität und Vertraulichkeit**, d.h. die Daten müssen angemessen vor dem Zugriff Dritter, vor Verlust und Zerstörung geschützt werden.

Die **Rechtmäßigkeit** ist hierbei besonders zu erklären: Personenbezogene Daten müssen immer auf rechtmäßige Weise, nach bestem Wissen und Gewissen und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (vgl. Art. 5, Abs. 1, Buchstabe a, DSGVO). Das bedeutet, dass die Datenverarbeitung grundsätzlich verboten ist, und Ausnahmen nur aufgrund von Rechtsgrundlagen erlaubt sind. Die entsprechenden **Kriterien der Rechtmäßigkeit der Datenverarbeitung** listet Art. 6 DSGVO auf: Daten dürfen dann verarbeitet werden, wenn min. eines der folgenden Kriterien (sog. Erlaubnistatbestände) erfüllt ist:

- Verarbeitung für die Erfüllung vertraglicher Zwecke;
- Erfüllung rechtlicher Pflichten;
- Schutz lebenswichtiger Interessen;
- Öffentliches Interesse;
- Wahrung berechtigter Interessen, sofern nicht die Grundrechte oder Interessen der betroffenen Person überwiegen. Hier ist davon auszugehen, dass ein gewisses, minimales Maß an Datenverarbeitung für die Arbeit von Fachkräften der Jugendsozialarbeit unerlässlich ist, bspw. für Projekte, Dokumentationen, Supervisionen, Teambesprechungen etc.



Eine mögliche Auslegung des Kriteriums »Wahrung berechtigter Interessen« ist die Abwägung zwischen Interessen der Fachkräfte (Ausführung der Arbeit, z. B. Beratung, Hilfe, Unterstützung für die Klient\*innen) und den Interessen der Klient\*innen (z. B. Schutz ihrer persönlichen Daten; aber auch: Unterstützung durch Jugendsozialarbeiter\*innen erhalten). Dies kann so ausgelegt werden, dass das Verarbeiten personenbezogener Daten von Klient\*innen durch Fachkräfte rechtmäßig sein kann. Diese Frage muss jedoch individuell **trägerintern abgewogen** werden und auch hier muss der **Prozess der Abwägung und seine Ergebnisse so weit wie möglich dokumentiert** werden. Diese Abwägung kann zum Ergebnis haben, dass bspw. die Nutzung von WhatsApp für die allgemeine Kommunikation mit Adressat\*innen bzw. Klient\*innen die niedrighschwellige, lebenswelt- und sozialraumorientierte Arbeit ermöglicht, die ohne die Präsenz von Jugendsozialarbeiter\*innen in diesem Medium nicht möglich wäre. Falls ein Träger zu dem Schluss kommt, dass die »Wahrung berechtigter Interessen« zutrifft, ist es möglich, auch ohne explizite Einverständniserklärung der Klient\*innen bestimmte Daten (z. B. Gesprächsinhalte/-protokolle aber auch persönliche Daten wie Name, Adresse, Alter) zu verarbeiten und zu speichern. Wichtig ist dann, die Daten bestmöglich zu anonymisieren, sie nicht auf fremden Servern zu speichern, eigene Endgeräte zu schützen (z. B. mit sicheren Passwörtern) und Löschfristen festzulegen sowie diese einzuhalten. Auch wenn gemäß Art. 6 Abs. 1 f) DSGVO die Verarbeitung der personenbezogenen Daten somit ohne eine explizite Einverständniserklärung rechtmäßig ist, ist es weiterhin angebracht und sinnvoll, die Klient\*innen zu **fragen** oder wenigstens darüber zu **informieren**, dass Daten verarbeitet oder gespeichert werden, um die Zusammenarbeit **transparent** und vertrauensvoll zu gestalten.

Ist keines der o. g. Kriterien erfüllt, muss eine explizite **Einwilligung** zur Datenverarbeitung der betroffenen Personen vorliegen. Diese sollte schriftlich erfolgen, um die Einwilligung später nachweisen zu können.

### Mehr Informationen

Die DSGVO selbst ist prinzipiell verständlich geschrieben. Darüber hinaus gibt es bereits Publikationen, die die Grundsätze der Datenverarbeitung für die Jugend(sozial)arbeit und die Inhalte und Anforderungen der DSGVO insgesamt umfassend aufbereiten. Besonders empfohlen sei hierzu die Publikation »Die DSGVO – Datenschutz in der Jugendarbeit« vom LJR Brandenburg und dem Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e.V. von 2019.

## Vier grundlegende Schritte für die datenschutzkonforme Arbeit

### Geräte

Unabhängig von den hier aufgezählten Schritten gilt: Jede Fachkraft sollte mit einem Dienst-Smartphone ausgestattet sein, um eine Trennung zwischen beruflicher und privater Kommunikation ermöglichen zu können und den Schutz der Daten von Klient\*innen und Jugendsozialarbeiter\*innen zu gewährleisten. Alle Geräte müssen mit sicheren Passwörtern geschützt werden, um den Zugriff Dritter auf alle auf den Geräten vorhandenen Daten zu verhindern.

### I. Anlegen und Pflege eines Verarbeitungsverzeichnisses

Das wichtigste Element zur Entwicklung von datenschutzsicherer Arbeit ist die **transparente und ausführliche Dokumentation über Tätigkeiten in der Erhebung und Verarbeitung** von Daten. Art. 30 DSGVO sieht vor, hierfür ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Mithilfe dieses Verzeichnisses werden alle Verarbeitungen von Daten standardisiert sowie Verantwortlichkeiten festgelegt und können so bspw. durch Prüfer\*innen nachvollzogen werden. Das Verzeichnis muss unter anderem alle verwendeten Plattformen und Tools, eine Erläuterung der erhobenen Daten, den Zweck der Erhebung bzw.

der Datenspeicherung und eine Löschfrist auflisten. Die Handreichung »Die DSGVO – Datenschutz in der Jugendarbeit« stellt übersichtliche Informationen zu Inhalten des entsprechenden DSGVO-Artikels zusammen. Dieses Verzeichnis ist bspw. bei Verwendung eines elektronischen Lohnbuchhaltungssystems vorgesehen und deshalb i. d. R. beim Träger bereits angelegt.

### **Verzeichnis der Verarbeitungstätigkeiten**

Ein Verarbeitungsverzeichnis kann bspw. als Excel-Tabelle angelegt und geführt werden. Muster für das Anlegen eines Verarbeitungsverzeichnisses gibt es im Internet. Auch die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder stellt gemeinsame Muster zur Verfügung. Eine detaillierte Anleitung für die Einführung und Umsetzung bietet Bitkom e.V. in der Handreichung »Das Verarbeitungsverzeichnis«.

Die Verantwortung für das Erstellen und Führen des Verarbeitungsverzeichnisses sollte bei dem\*der **Datenschutzbeauftragten**, ggf. gemeinsam mit der Geschäftsführung, liegen. Ein\*e Datenschutzbeauftragte\*r ist einerseits verantwortlich für die Unterrichtung der Mitarbeitenden zum Datenschutz, für die Dokumentation und generelle Fragen zum Datenschutz und andererseits direkte Ansprechperson für Externe (z. B. Datenschutzbehörden) – die Aufgaben sind im Art. 39 DSGVO geregelt.

## **II. Datenschutz-Check vor dem Beginn der Nutzung eines Tools / Dienstes**

Für eine sichere Arbeit ist **Transparenz** und eine **offene, klare Kommunikation und Dokumentation zum Umgang mit Datenschutz** essenziell. Dazu gehört es, Fragen des Datenschutzes schon vor der Aufnahme der Arbeit mit sozialen bzw. digitalen Medien zu beachten. So müssen Dienste bzw. Plattformen geprüft und Datenschutzfragen, Dokumentationen und Vorgehensweisen geklärt werden.

Ein sinnvoller Schritt zu bestmöglicher datenschutzgerechter Arbeit ist die Durchführung eines **Datenschutz-Checks**. So werden datenschutzrelevanten Fragen vor Beginn der Nutzung eines Tools bzw. Dienstes bewusst reflektiert und die Überlegungen werden dokumentiert. Die aktive Auseinandersetzung mit dem Datenschutz vor Beginn der Nutzung ist ein wichtiger Schritt zur DSGVO-Konformität und die

transparente Dokumentation dieser Auseinandersetzung sichert den Träger im Falle einer Prüfung durch Datenschutzbehörden ab. Die Fragen **sollten von bzw. gemeinsam mit dem\*der Datenschutzbeauftragten beantwortet werden:**

**Frage 1:** Verarbeitet die ausgewählte Social-Media-Plattform/Messenger-Dienst personenbezogene Daten?

**Frage 2:** Zu welchen Zwecken wird die Social-Media-Plattform/Messenger-Dienst benötigt?

**Frage 3:** Kann der Zweck nicht ohne Einsatz dieser Social-Media-Plattform/Messenger-Dienst erreicht werden? Falls nein, warum?

**Frage 4:** Bietet die Social-Media-Plattform/Messenger-Dienst einen Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO (Data Protection Agreement) oder eine Vereinbarung über gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO an?

### **Auftragsverarbeitungsvertrag (AVV)**

Es ist hilfreich – wenn auch nicht zwingend erforderlich – wenn ein AVV abgeschlossen werden kann. Daher ist es sinnvoll, bei einem Dienst einen solchen Vertrag anzufordern und dies zu dokumentieren, um die Bemühung nachzuweisen. Häufig ist der AVV Teil der Nutzungsbedingungen und wird durch die Registrierung und die Einwilligung in die Rahmenbedingungen automatisch unterzeichnet (dies ist der Fall bei Diensten wie z. B. Zoom und Facebook). Weitere Informationen hierzu gibt es z. B. im Handbuch »Die DSGVO – Datenschutz in der Jugendarbeit« auf S. 40 oder bei Blogmojo (inkl. einer Liste von Plattformen, die einen AVV anbieten).

**Frage 5:** Verarbeitet die Social-Media-Plattform/der Messenger-Dienst personenbezogene Daten in Ländern außerhalb der EU, sitzt außerhalb der EU oder setzt selbst Unterauftragnehmer ein, auf die das zutrifft?

**Frage 6:** Verfügt der Dienst über Einstellungs- oder Auswahlmöglichkeiten, welche die Verarbeitung von Daten möglichst einschränken und möglichst sicher gestalten? Falls ja, welche Optionen bestehen und falls sie nicht gewählt werden, begründen Sie bitte, warum.

Die Antworten können abhängig vom Kommunikationskanal sehr verschieden ausfallen, da das Ziel der Beantwortung eine transparente und ausführliche Auseinandersetzung mit dem Datenschutz ist. Das bedeutet: Wenn die Nutzung eines bestimmten Dienstes nach der dokumentierten Beantwortung der o.g. Fragen als notwendig für die Erfüllung des Auftrags der Fachkräfte erachtet wird, muss im Träger bzw. Projekt besprochen werden, welche Möglichkeiten es gibt, einen größtmöglichen Schutz der personenbezogenen Daten der Adressat\*innen bzw. Klient\*innen zu gewährleisten. Die Antworten auf die Fragen 4 (Auftragsverarbeitungsvertrag) und 6 (Optionen / Einstellungen zur Einschränkung der Datenverarbeitung) können anschließend bei der Nutzung des Tools / Dienstes dabei helfen, personenbezogene bzw. sensible Daten bestmöglich zu schützen.

Wenn der Träger / das Projekt o.ä. sich für die Nutzung eines Tools, einer Plattform, eines Dienstes o.ä. entscheidet, muss dieser in das Verzeichnis aufgenommen werden.

### III. *Anpassung der eigenen Datenschutzerklärung*

Der nächste Schritt ist die Anpassung der eigenen **Datenschutzerklärung**. Die Nutzung von Online-Plattformen muss in der Datenschutzerklärung des Trägers bzw. des Projektes erwähnt und es muss jeweils erklärt werden, in welcher Form Daten erhoben, verarbeitet und genutzt werden können. Zudem müssen die jeweiligen Websites der Plattformen sowie die Datenschutzerklärungen und Opt-Out-Regelungen – um dem jeweiligen Dienst die Datenverarbeitung zu untersagen – verlinkt werden.

## Datenschutzerklärung

I.d.R. muss eine gültige Datenschutzerklärung auf der eigenen Website veröffentlicht sein. Eine Hilfestellung bietet ein Papier der Landesdatenschutzbeauftragten von Niedersachsen mit Informationen für Website-Betreibende. Hier wird auch erklärt, welche Informationen darin grundsätzlich enthalten sein müssen und wichtige Hinweise gegeben. Beispielsweise müssen alle Informationen laut Art. 12 DSGVO »in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache« vermittelt werden – was in der Arbeit mit Kindern und Jugendlichen besonders zu beachten ist.

### IV. Datenschutzerklärung und Impressum in Online-Präsenzen aufführen

Der vierte Schritt beinhaltet die **Anpassung der eigenen Online-Präsenzen** (vor allem Arbeitsprofile) der Fachkräfte, d. h. die datenschutzkonforme Angabe der eigenen Daten, einer Datenschutzerklärung und eines Impressums im Arbeitsprofil. Nicht nur aus Gründen des Datenschutzes, sondern auch zur Wahrung der professionellen Transparenz ist solch ein Umgang mit den eigenen Profilen sinnvoll: die Angaben helfen Klient\*innen sowie deren Umfeld, professionelle Profile erkennen und überprüfen zu können. Die Angaben müssen immer leicht auffindbar sein und direkt und korrekt zum Träger und den Datenschutzregeln verlinken.

Das folgende Kapitel gibt Hilfestellungen für die Erstellung eines Arbeitsprofils durch Jugendsozialarbeiter\*innen auf verschiedenen Plattformen. Auch die praktische Umsetzung der Einbindung von Impressum und Datenschutzerklärung werden beschrieben.

## Hinweise für die Erstellung von Arbeitsprofilen in sozialen und digitalen Medien

Spätestens durch die offizielle Forderung von Schutzkonzepten durch Jugendämter ist es wichtig, Arbeitsprofile so transparent wie möglich zu gestalten. Das beinhaltet die Angabe von einigen Daten: Klarname des\*der Inhaber\*in des Accounts, konkrete Informationen zur Tätigkeit, Name des Trägers und/oder des Projektes und ggf. Logos des Projektes/des Trägers (sowie ggf. von Fördergebern). Darüber hinaus muss sowohl eine **Datenschutzerklärung** als auch ein **Impressum** verlinkt

werden. Diese Links müssen korrekt ans Ziel weiterleiten, anklickbar und sog. »sprechende Links« sein: das Wort *Impressum* bzw. *Datenschutzerklärung* muss leicht erkennbar im Link stehen und direkt bei Aufruf der Seite/des Profils erkennbar sein. Die Angabe dieser Daten kann auf den jeweiligen Plattformen auf unterschiedliche Weise umgesetzt werden, um eine größtmögliche Transparenz zu gewährleisten.

**Facebook** bietet die Möglichkeit, mehrere Links in der Profilbeschreibung anzugeben, sodass sowohl Datenschutzerklärung und Impressum direkt sichtbar sind. Bei **Instagram** ist es allerdings nur möglich, einen einzelnen anklickbaren Link in der »Biografie« anzugeben. Hierfür gibt es mehrere Lösungen: Viele Behörden nutzen für multiple Verlinkungen den US-amerikanischen Dienst **Linktree**. Linktree bietet die Möglichkeit, über die Angabe eines Links in einem Profil auf mehrere Links zu Dokumenten in einem Raum zuzugreifen (Abb. 2).

Da Linktree in den USA gehostet wird, kann die Nutzung ggf. als problematisch eingeschätzt werden. Um dieses Problem zu umgehen, ist auch die Verlinkung zu einer Übersichtsseite (z. B. auf der Website des Trägers/des Projektes) mit Angaben zu Impressum und Datenschutzerklärung möglich und ebenso effektiv (Abb. 3).

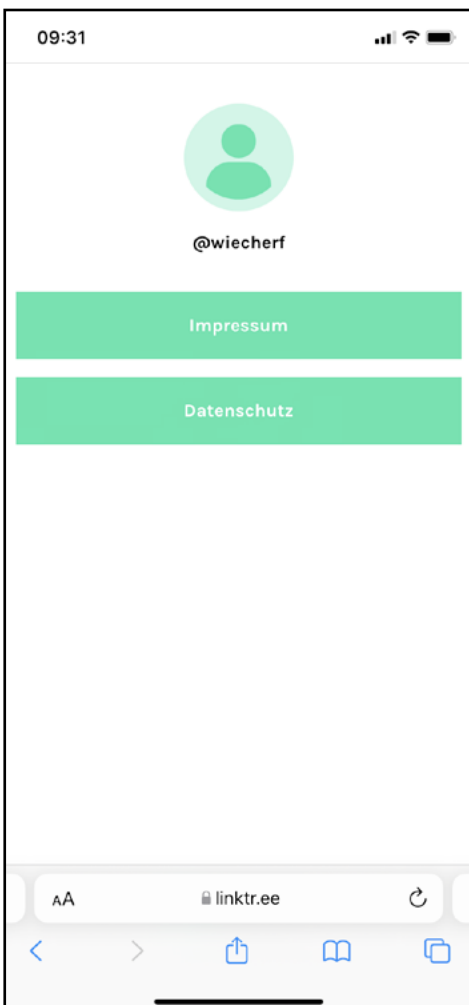


Abbildung 1: Beispiel einer Aufführung von Links in Linktree (Übersichtsseite zur Verlinkung in einem Arbeitsprofil)

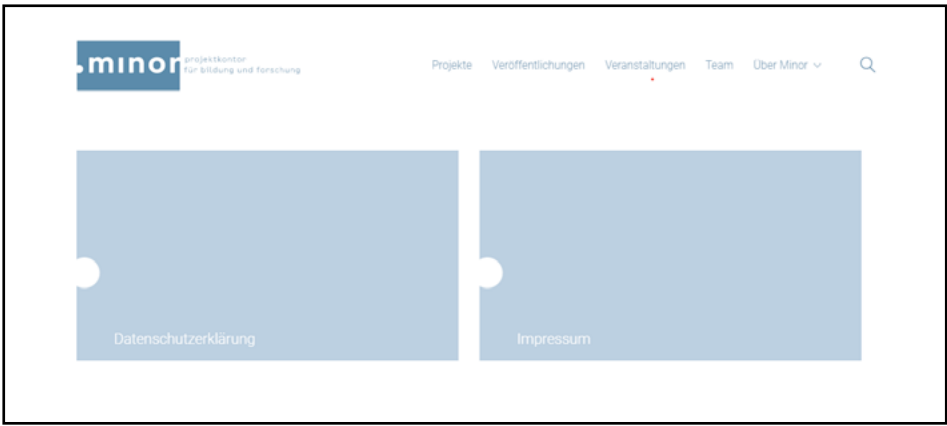


Abbildung 2: Beispiel einer Verlinkung von Datenschutzerklärung und Impressum auf der trägereigenen Website.

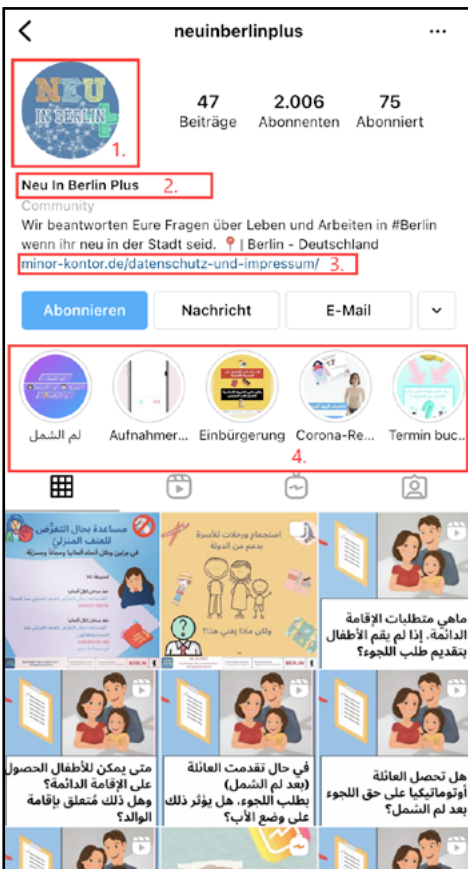


Abbildung 3: Screenshot eines Instagram-Accounts des Projektes »Neu in Berlin Plus« © Minor

Eine dritte Variante bspw. für Instagram ist die Verlinkung von Impressum und Datenschutzerklärung in einem **Storybeitrag**. Da diese Beiträge für die Zielgruppe nur 24 Stunden sichtbar sind, ist es wichtig, den Beitrag in einem **Highlight** zu speichern und dieses dementsprechend zu benennen.

Abbildung 3 zeigt ein Beispiel eines Arbeitsprofils inklusive wichtiger Elemente. Markierung 1 zeigt das Profilbild, hier ein Logo des Projekts. Markierung 2 beinhaltet den Namen des Projektes, hier ist



der ausgeschriebene Name des Projekts erforderlich. In Markierung 3 befindet sich der »sprechende Link« für eine Übersichtsseite mit Datenschutzerklärung und Impressum des Trägers. Die Highlights sind in Markierung 4 zu finden, hier könnten alternativ die nötigen Angaben aus Abschnitt 3 (Impressum, Datenschutzerklärung) verlinkt und dementsprechend benannt werden.

Für die Kommunikation über **WhatsApp** im Rahmen der Jugendsozialarbeit sollte von Seiten der Fachkräfte nach Möglichkeit WhatsApp Business genutzt werden. Diese Version des Dienstes ermöglicht viele Einstellungen, die zu einer transparenten Arbeit beitragen – u. a. das Einstellen von Links zum Impressum und der Datenschutzerklärung sowie weiterer Angaben zum Träger und der Fachkraft. Das Projekt »DiMe« bietet hierzu eine separate Arbeitshilfe zur Erstellung eines WhatsApp-Business-Accounts.

## Umgang mit besonders sensiblen Daten

Aufgrund der Arbeit mit oftmals sehr persönlichen Informationen der Klient\*innen beschäftigt sich diese Arbeitshilfe mit **besonders zu schützenden personenbezogenen Daten** und einem möglichen Umgang mit diesen. Über »personenbezogene Daten« hinaus erwähnt die DSGVO in Art. 9 sog. »**besondere Kategorien personenbezogener Daten**« – d. h. Daten, die besonders zu schützen sind. In Art. 9 Absatz 1 heißt es: »Die Verarbeitung personenbezogener Daten, aus denen die rassische<sup>1</sup> und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.« Im Kontext der Jugendsozialarbeit können diesen Kategorien bspw. auch strafrechtlich relevante Informationen hinzugefügt werden, die aus individual-moralischer und/oder professioneller Perspektive besonders schützenswert sein können.

Bei Gesprächsinhalten oder Informationen zu solchen Kategorien ist die Überführung der Konversation auf einen sicheren Kommunikationskanal besonders erstrebenswert bzw. nötig. Diese Informationen – und damit die Klient\*innen selbst – müssen schließlich auch aus professioneller Sicht ganz besonders vor der Einsicht bzw. dem Zugriff

1 Die Reproduktion des Begriffs »rassisch« betrachten wir als problematisch. Da der Gesetzes text der DSGVO diesen Begriff aber hier verwendet, wird dieser im Zitat wiedergegeben.

durch Dritte geschützt werden. Die Gefahr dazu besteht nicht nur bei der Nutzung nicht-DSGVO-konformer Messenger oder Plattformen, sondern auch, indem Backups von Konversationen oder Fotos automatisch in Clouds gespeichert werden, wenn ein Endgerät geteilt wird oder verloren geht oder aber auch, wenn Inhalte durch die Jugendlichen absichtlich oder aus Versehen in Gruppen, Statusupdates oder öffentlichen Profilen geteilt werden.

Die sichersten Kommunikationswege sind solche, die garantiert nicht nachverfolgt werden können, also analoge Treffen – z. B. Spaziergänge oder Beratungsgespräche in geschützten Räumen. Sollte dies nicht in Frage kommen, muss auf einen digitalen Weg zurückgegriffen werden. Die diversen Online-Plattformen unterscheiden sich hier hinsichtlich ihrer Datensicherheit. Als besonders sicher sind die Messenger **Wire** und **Signal** einzustufen. Mehr zu sicheren bzw. unsicheren Plattformen, Vergleichen und Details sind in der DiMe-Arbeitshilfe »Digitale Kommunikationstools für die (aufsuchende) Jugendsozialarbeit« zu finden. Während »selbstlöschende Nachrichten« wie bei Snapchat oder optional bei WhatsApp eine Lösung zu bieten scheinen, können diese z. B. durch Screenshots oder Weiterleitungen vor dem Löschen gesichert werden.

Die zentrale Frage ist: **Wann und wie kann die Kommunikation auf einen sicheren Kanal übergeleitet werden?**

Generell ist die Änderung des Kommunikationskanals eine Abwägungsfrage zwischen dem Risiko des Kontaktabbruchs und dem Wert einer sicheren, vertraulichen Kommunikation und dient insbes. dem Schutz der Klient\*innen sowie der Fachkräfte vor dem Zugriff Dritter auf persönliche Informationen. Zum Abwägungsprozess sollte gehören, das Gegenüber über potenzielle Gefahren und Konsequenzen des Teilens von sensiblen Daten auf unzureichend geschützten Plattformen aufzuklären. Darüber hinaus ist es ratsam, im Träger bzw. Projekt eine gemeinsame Strategie zu besprechen und dies zu dokumentieren. Hier können sichere Kommunikationswege (bspw. Wire (Messenger), Telefonate, Face-to-Face-Treffen) und die Überführung in diese besprochen werden. Außerdem sollten Richtlinien für den Umgang mit Extrem- oder Notsituationen besprochen werden. Diese können bspw. thematisieren, zwischen physischer und psychischer Sicherheit der Klient\*innen und dem Datenschutz abzuwägen: hier kann die Rechtmäßigkeit der Datenverarbeitung (d. h. die Einhaltung der DSGVO) durch die oben aufgeführte »Wahrung berechtigter Interessen« oder auch den »Schutz lebenswichtiger Interessen« gegeben sein. Ein Beispiel hierfür wäre, dass Klient\*innen in akuten Notsituationen über WhatsApp unterstützt werden, selbst wenn Informationen aus dem Bereich der »besonderen Kategorien personenbezogener Daten« über-

mittelt und damit potenziell bspw. durch WhatsApp verarbeitet werden können. Sinnvoll ist die **Dokumentation** dieser (gemeinsamen) Entscheidungen und Prozesse, um Transparenz und Nachvollziehbarkeit zu gewährleisten und der DSGVO zu entsprechen.

## Selbstschutz der Fachkräfte

Wie auch in der analogen Arbeit, muss der Selbstschutz der Fachkräfte gewährleistet werden. Problematisch kann etwa der Fall sein, wenn Klient\*innen der Fachkraft strafrechtlich relevante Inhalte zukommen lassen: mit dem Besitz bestimmter Daten (bspw. kinderpornografische Inhalte oder Gewaltdarstellungen) macht sich die Fachkraft ggf. strafbar. In diesem Fall sollte die Fachkraft auf die Problematik des Teilens hinweisen, alternative Kommunikationsformen anbieten und ggf. dazu auffordern, diese Daten nicht zu übermitteln. Im Einzelfall kann es nötig sein, den\*die Klient\*in zu blockieren. So kann sich die\*der Jugendsozialarbeiter\*in vor Konsequenzen schützen, die beim Besitz von sensiblen Daten einer anderen Person oder aber auch von allgemein strafrechtlich relevanten Bildern / Videos etc. folgen können.

## Jugendliche für Datenschutz sensibilisieren

Da der digitale Raum zu einer relevanten Lebenswelt Jugendlicher geworden ist, müssen diese für Gefahren und Konsequenzen des eigenen Verhaltens und insbes. der Preisgabe von Informationen über sich selbst im Netz sensibilisiert werden. Für mögliche Herangehensweisen wurden beim Fachtag Erfahrungsberichte und Ideen der Streetworker\*innen gesammelt.

Dabei zeigt die Erfahrung, dass auch dieses Thema am besten in einem offenen und transparenten Gespräch mit Klient\*innen besprochen wird. Dabei sind authentische und ehrliche Erklärungen (z. B. »In meiner Welt ist das nicht okay«, »Aufgrund diesem und jenem Post ist das und das passiert«) hilfreich. Auch können eigene Erfahrungen bzw. die Erfahrungen mit anderen Jugendlichen mit einfließen. Um Selbstreflexion der Jugendlichen anzustoßen, können Erzählungen aus eigener Perspektive helfen (z. B. »Auf mich hat das so und so gewirkt«). Bei Sprachbarrieren kann die Kommunikation ggf. mit Google-Übersetzer einen echten Mehrwert bieten.

Prinzipiell ist überdies wichtig zu beachten: Klient\*innen sollten nie von einer Fachkraft dazu *aufgefordert* werden, personenbezogene Daten über einen (potenziell) nicht-DSGVO-konformen Kanal zu übermitteln. In der Praxis lässt sich dies z. B. umsetzen, indem immer auch analoge Gesprächsräume, Telefonate und/oder DSGVO-konforme digi-

tale Alternativen angeboten werden und offen sowie verständlich über den Datenschutz der Plattformen informiert wird.

### **Flyer für Jugendliche**

Einen Einstieg in das Verständnis der AGBs und Datenschutzbestimmungen beliebter Plattformen bieten beispielsweise die Flyer von klicksafe, die wichtige Inhalte für Jugendliche verständlich zusammenfassen.

### **Fazit**

Der korrekte Umgang mit Datenschutz stellt in der digitalen Jugendsozialarbeit eine Herausforderung dar. In der Praxis ist es für die Arbeit mit den Klient\*innen und das Aufrechterhalten der Kommunikation für viele Fachkräfte nicht möglich, die Nutzung von populären Plattformen auszuschließen. Gleichzeitig entsprechen viele Plattformen und Messenger-Apps der DSGVO nicht (vollständig). Um dennoch den bestmöglichen Schutz der Daten der Jugendlichen sicherzustellen, ist es essenziell, die Arbeit so transparent wie möglich zu gestalten. Das bedeutet, Entscheidungen auf Basis der DSGVO, der Bedarfe und Lebensrealitäten der Klient\*innen und der eigenen professionellen Standards und Möglichkeiten abzuwägen und ausreichend zu dokumentieren.

Die in dieser Arbeitshilfe beschriebenen Schritte und Maßnahmen können nicht für eine komplette Absicherung garantieren. Sie sollen Träger und Fachkräfte jedoch dabei unterstützen, einen verantwortungsvollen und professionellen Umgang mit dem Datenschutz im Rahmen ihrer Arbeit mit und in den Lebenswelten ihrer jugendlichen Klient\*innen zu finden.

### **Wo finde ich mehr?**

Hilfreiche, umfassende Publikationen zum Thema Datenschutz in der Jugend(sozial)arbeit sind die Handreichung »Die DSGVO - Datenschutz in der Jugendarbeit« des Landesjugendrings Brandenburg und des Fachverbands Jugendarbeit / Jugendsozialarbeit Brandenburg e. V. und »Digital.Total?!« Handreichung - Zum Umgang mit Social Media in der Mobilen Jugendarbeit der LAG Mobile Jugendarbeit / Streetwork Baden-Württemberg e. V. Die öffentlichen Datenschutzinstanzen haben das Informationsangebot www.datenschutz.de als »virtuelles Datenschutzbüro« eingerichtet: hier können u. a. verschiedene Leitfäden bspw. zum Datenschutz auf dem Smartphone heruntergeladen werden.

## **Impressum**

Minor – Projektkontor für Bildung und Forschung gGmbH 2021

Text und Daten: Freyja Wiechers, Laura Ballaschk

»DiMe – digitale Methoden der (aufsuchenden) Jugendsozialarbeit« ist ein Projekt von



Alt-Reinickendorf 25

13407 Berlin

Tel.: +49 (0)30 457 98 95 21

E-Mail: [minor@minor-kontor.de](mailto:minor@minor-kontor.de)

[www.minor-kontor.de](http://www.minor-kontor.de)

<https://minor-kontor.de/dime/>

Das Projekt »Digitale Methoden der (aufsuchenden) Jugendsozialarbeit« (DiMe) wird gefördert und unterstützt durch

**BERLIN GEGEN  
GEWALT**

**Landeskommission  
Berlin gegen Gewalt**



© Minor – Projektkontor für Bildung und Forschung im November 2021